This document is scheduled to be published in the
Federal Register on 12/20/2023 and available online at
https://federalregister.gov/d/2023-27948, and on **https://govinfo.gov**

9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0027]

Request for Information on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software"

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: Notice; request for information.

SUMMARY: CISA requests input from all interested parties on the white paper "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software."

DATES: Written comments are requested on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may send comments, identified by docket number CISA-2023-0027, by following the instructions below for submitting comments via the Federal eRulemaking Portal at http://www.regulations.gov.

Instructions: All comments received will be posted to https://www.regulations.gov, including any personal information provided. If you cannot submit your comment using https://www.regulations.gov, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this notice for alternate instructions. For detailed instructions on sending comments and additional information on the types of comments that are of particular interest to CISA, see the "Public Participation" heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Documents: The draft white paper titled “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software” is available at https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.

Docket: For access to the docket and to read comments received, go to https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Megan Doscher, 202-975-4911, SecureByDesign@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION:

I. Public Participation

Response to this RFI is voluntary. Interested persons are invited to comment on this notice by submitting written data, views, or arguments using the method identified in the **ADDRESSES** section above. All members of the public including, but not limited to, specialists in the field, academic experts, members of industry, public interest groups, and those with relevant economic expertise are invited to comment. The draft white paper titled “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software” is available at https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.

Instructions: All submissions must include the agency name and Docket number for this notice. Comments may be submitted electronically via the Federal e-Rulemaking Portal. To submit comments electronically:

1. Go to *www.regulations.gov* and CISA-2023-0027 into the search field.
2. Click on the “Comment Now!” icon.
3. Complete the required fields.
4. Enter or attach your comments.

All submissions, including attachments and other supporting materials, will become part of the public record and may be subject to public disclosure. CISA reserves the right to publicly publish relevant and unedited comments in their entirety. Do not include personal information such as account numbers, Social Security numbers, or the names of other individuals. Do not submit confidential business information or otherwise sensitive or protected information. All comments received shall be posted to *http://www.regulations.gov*. Commenters are encouraged to identify the number of specific topic(s) they are addressing.

II. Background

Products that are secure by design are those where the security of the customers is a core business goal, not a technical feature. Secure by design products start with that goal before development begins. Secure by default products are secure and ready to use "out of the box" with little to no necessary configuration changes; moreover, the security features are available without any additional costs. Together, these two concepts move much of the burden of staying secure to the manufacturers and reduce the chance that the customer will fall victim to security incidents resulting from misconfigurations, insufficiently fast patching, or other common issues.

Consequently, it is crucial for software manufacturers to make secure by design and secure by default the focal points of product design and development processes. The white paper strongly encourages every software manufacturer to build products in a way that reduces the burden of cybersecurity on customers. To achieve this outcome, software manufacturers are urged to evolve their design and development programs to permit only secure by design and secure by default products to be shipped to customers.

The white paper identifies three core principles to guide software manufacturers in building software security into their design processes prior to developing, configuring, and shipping their products to customers:

1. *Take Ownership of Customer Security Outcomes*: Software manufacturers should take ownership of their customers' security outcomes and evolve their products

accordingly. Software manufacturers should invest in product security efforts that include application hardening, application security features, and application default settings.

2. *Embrace Radical Transparency and Accountability*: Software manufacturers should pride themselves in delivering safe and secure products. Transparency will help convey what "good" looks like, and that information will benefit the defenders more than our adversaries.
3. *Lead From the Top*: Build organizational structure and leadership to achieve these goals. Senior leaders must make security a business priority and not just a technical matter. Internal incentives and culture must support security as a design requirement. While technical subject matter expertise is critical to product security, senior leaders are the primary decision makers for implementing change in an organization.

CISA acknowledges that security by design is not easy. For example, implementing a secure software development lifecycle (SDLC) is a difficult task and takes time; smaller software manufacturers may struggle to implement many of these suggestions. As more organizations focus their attention on secure software development, there is room for innovations that will narrow the gap between the larger and smaller software manufacturers. Furthermore, engineering teams will be able to establish a new, steady-state rhythm in which security is built into the design and takes less effort to maintain.

The "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software" white paper identifies a path forward for implementing security by design and security by default into the SDLC, placing the burden of cybersecurity on manufacturers instead of customers. The white paper explores the benefits and challenges of applying the three secure by design principles. In doing so, the white paper outlines the requirements and activities necessary for software manufacturers to adopt a secure by design philosophy. An updated version of the white paper was published on October 16, 2023.[1]

III. Additional Topics for Commenters

This white paper is part of a broader campaign across CISA and the federal government to encourage technology manufacturers to prioritize security in their development processes. For future iterations of guidance, CISA also seeks additional information on the economics of secure development, particularly as compared with the cost of incident response. Additionally, for use in future guidance, CISA seeks information from the public describing how security could be more fully integrated into computer science and software development courses of study.

In addition to comments on the white paper, CISA seeks comments and information on the following related topics:

1. **Incorporating security into the SDLC.**
   a. Among the many tactics for weaving security into the SDLC, which tactics are the most effective? How is that impact measured?
   b. What actions in the white paper are respondents taking, and what measured results are they seeing? Have respondents publicly documented these actions and their results and, if so, where?
   c. Smaller software manufacturers report that they struggle to implement the tools and practices that larger manufacturers can implement. What are some examples of smaller software companies that have implemented well-lit paths to reduce product vulnerabilities?
   d. What are some best practices that smaller software companies can adopt?

[1] The updated white paper "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software" can be found at https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.

e. What improvements are needed to allow most small software manufacturers to build and maintain software that is secure by design?

f. What are some examples of companies that invest in continuous security education for software developers? How much do these programs cost, and what are the results?

2. **Education**. University-based computer science degree programs must manage many priorities, including research, student demand, faculty and tenure requirements, and curriculum design. Security is often relegated to an elective, rather than a core component of the program. Online education programs, which offer a viable and convenient pathway toward a degree or a specialized skill set in computer science or software development, have similar outcomes, though perhaps for different reasons.

   a. What are some examples of commercial entities signaling their demands to universities for knowledge of security and secure coding in graduates of computer science programs? Is knowledge of security evaluated during the hiring stage, or are employees reskilled after being hired?

   b. What are some examples of higher education incorporating foundational security knowledge into their computer science curricula? How did the universities incorporate the knowledge and what were some results? Did students demand additional security training, or were they resistant? Were students able to differentiate their skillsets based on this knowledge and experience?

   c. How can current or prospective students for online computer science or coding education programs signal their demands for security? What are some actions that online programs can take to incentivize companies to develop content with integrated security principles that are hosted on their platforms?

3. **Hardening/loosening guides**. Hardening guides are supplements to installation guides that help customers configure and deploy a product with a stronger security posture than the product's defaults would create.
    a. What are some best practices for hardening guides? What are some good examples?
    b. How do software manufacturers decide on their products' default configurations, and how do those decisions affect the length and complexity of the hardening guide?
    c. What are some examples of products that have something closer to a "loosening guide?"
    d. How do companies decide which staff members author the hardening/loosening guides, and how much cybersecurity experience do those members have? What are some best practices that more companies should adopt?
    e. Are there examples of products that offer automated hardening mechanisms, such as in installation scripts or in real-time when configuring settings, rather than in a supplemental document?
    f. What are customers' experiences with multiple hardening guides across a large tech stack?
4. **Economics of implementing secure by design practices**. Just as cars with crumple zones and air bags may cost their manufacturers more to build than cars without such safety mechanisms, developing secure by design products is likely to cost the software manufacturer more than if the manufacturer did not emphasize

product and customer security. CISA requests additional information about the magnitude and sources of these costs.

   a. What types of costs do software manufacturers incur as they implement and mature their secure by design programs? Examples might include developer training, security analysis tools, migrating to memory safe languages (MSL), and vetting the security of open-source libraries.
   b. How much are these costs, typically; to what extent are they absorbed by manufacturers; and to what extent are they passed along to consumers through price increases?
   c. Which secure by design practices are the most effective, and what voluntary guidance should CISA consider issuing to encourage those practices?

5. **Economics of software vulnerabilities**. Software vulnerabilities cost software manufacturers and their customers time, effort, and money. CISA seeks additional information about how software manufacturers measure these costs and how manufacturers respond as costs fluctuate.

   a. Impact of vulnerabilities on software manufacturers.
      i. How do software manufacturers measure their costs for each vulnerability?
      ii. Do software manufacturers measure the financial impact of vulnerabilities over time? If so, what are some examples of common patterns that emerge?
      iii. What are the differences in the remediation costs associated with vulnerabilities discovered in-house compared to the costs associated with vulnerabilities found after customers have deployed the product?

iv. How do software manufacturers determine how to remediate vulnerabilities, e.g., whether to patch specific instances of a vulnerability versus making other changes to remove the class of vulnerabilities? Does the size of the company (small versus large) make a difference for these choices? Are there particular cost structures that warrant investments in removing the class of vulnerabilities rather than patching vulnerabilities upon subsequent discovery? What factors or considerations do software manufacturers use to determine the financial decision points?

v. Where in the software manufacturer's organization are tradeoffs made based on this financial data? Are these tradeoffs handled as technical matters or as business matters addressed by senior business leaders?

b. Impact of vulnerabilities on customers.

i. Do software manufactures calculate costs for consumers? If so, how do software manufacturers determine the average cost for customers to deploy software updates to mitigate a software vulnerability?

ii. How do software manufacturers determine the aggregate cost across all customers for patching?

6**.** **Economics of customer demand.** Software manufacturers generally implement the features customers ask for the most. There is a perception that customers are not asking for security in the products they buy.

a. In what ways do customers ask software manufacturers to make products more secure?

b. In what ways do customers ask for specific security features rather than asking for products that are secure by design?

c. How can customers measure the security of a product? Can they take that measurement and translate it into long-term costs to decision makers in a business?

d. What are the inhibitors to customers creating a strong demand signal that software should be secure by design?

7. **Field studies**. Field studies can illuminate how customers configure and use products in ways that may differ from the developer's expectations. For example, a field study might determine that a significant percentage of customers use unsafe settings when safer ones exist, thus putting them at risk, possibly without their knowledge.

   a. Do software manufacturers carry out such field studies? If so, what are some examples of software manufacturers that have implemented formal field studies, and how did those studies affect the design of future versions of that software? How did those studies affect the user experience of the security settings in line with how the software is supposed to function in different sectors (such as healthcare, K-12, etc.)?

   b. What are some best practices for conducting field studies and incorporating the results into the SDLC? Are field studies on the user experience of security settings and software function conducted and, if so, what are some best practices?

   c. What costs and benefits do field studies have for software manufacturers? For their customers?

8. **Recurring vulnerabilities**. In the news, we frequently see examples of software vulnerabilities for which effective mitigations have been available for years, or

even decades. Examples include hard-coded credentials, SQL injection vulnerabilities, and directory path traversal vulnerabilities.

   a. What are the barriers to eliminating recurring classes of vulnerability?

   b. How can potential customers determine which software manufacturers have been diligent in removing classes of vulnerability rather than patching individual instances of that class of vulnerability?

   c. What changes to the Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) programs might lead to more companies identifying recurring vulnerability types and investing to eliminate them?

9. **Customer upgrade reluctance**. When software manufacturers improve a product, perhaps by implementing a new security feature or network protocol, customers may need to act to take advantage of those improvements. However, customers do not always adopt those security improvements, particularly if the improvements cost them time or money.

   a. What are the primary barriers to customers investing in upgrades that should reduce their risk?

   b. What are some examples of security improvements where customer adoption was swift despite those barriers? What factors made customer upgrades more likely? How much did the software manufacturer need to invest in dollars or customer outreach to achieve broad adoption?

10**. Threat modeling**. Threat modeling is a technique used to identify assets and threats and to design, implement, and validate mitigations.

   a. What are some examples of threat models that software manufacturers have made public?

b. What are some best practices for publishing a high-level threat model that will demonstrate to customers that the software manufacturer has adopted a robust threat-modeling program as part of its SDLC?

11**. Charging for security features**. Companies often charge more for security features. Companies may choose to include security features only in higher-product tiers, or they may charge for it as a separate line item. For example, some software companies charge customers more when they want to use a single sign-on (SSO) service or if the customer wants access to all security related audit logs. CISA seeks additional information about how software manufacturers might decide to charge for a feature or to include it in the base price.

a. How do software manufacturers decide which pricing model is appropriate?

b. What considerations do they factor into their decision?

12**. Artificial Intelligence (AI)**. AI is software and therefore should adhere to the three secure by design principles.

a. What additional security considerations are necessary for the development of secure AI?

13**. Operational Technology (OT)**. OT systems can differ significantly from information technology (IT) systems. OT systems operate in different environments in which availability is the main priority. Unlike some IT systems that are refreshed or replaced every few years, some OT systems may operate in the field for a decade or more.

a. Which OT products or companies have implemented some of the core tenants of secure by design engineering?

b. What priority levels do customers place on security features and product attributes? What incentives would likely lead customers to increase their demand for security features, even if it costs more?

c. Where could targeted investments be made to raise and scale security levels across OT?

This notice is issued under the authority of 6 U.S.C. 652 and 659.

Eric Goldstein,
Executive Assistant Director for Cybersecurity,
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security.

[FR Doc. 2023-27948 Filed: 12/19/2023 8:45 am; Publication Date: 12/20/2023]